J. Algebra Comb. Discrete Appl.
4(2) • 197–206

Received: 12 June 2015
Accepted: 29 February 2016

Journal of Algebra Combinatorics Discrete Structures and Applications

Correspondence between steganographic protocols and error correcting codes

Research Article

M'hammed Boulagouaz, Mohamed Bouye

Abstract: In this work we present a correspondence between the steganographic systems and error correcting codes. We propose a new steganographic protocol based on 3-error-correcting primitive BCH codes. We show that this new protocol has much better parameters than protocols which we get from Hamming codes or from the 2-error-correcting primitive BCH codes, for high levels of incorporation.

2010 MSC: 94A60, 94B29, 94B40

Keywords: Steganographic protocol, Hamming distance, Linear correcting code, Covering radius, Parity matrix, BCH code

1. Introduction

The etymology of steganography is composed of two Greek words: "Stego" which means secret and "graphia" writing. Steganography is then the art of secret writing. More generally, we call steganography, the art of hide information in a carrier, so that is hidden information from to furtive eyes of anyone other than the sender and the recipient.

The field of information security grows and grows increasingly in recent spent decades. The development of systems for the protection of information has taken great interest as a subject of scientific research. Cryptographic protocols is the best acknowledged of such systems. However, new ideas emerged with force in recent years. Steganography is an old area that thanks to recent progress begins to play an important role as an alternative and more generally as a complement of cryptography. The advantage of steganography over cryptography is that steganography protects information like cryptography and it protects also communicating sources.

Error-correcting codes are important tools for the design of algorithms for steganography. They are used to hide information in an image and also to extract hidden information from the modified image.

M'hammed Boulagouaz (Corresponding Author), Mohamed Bouye; King Khalid University, Faculty of Sciences, B.P. 9004, Abha, Saudi Arabia (email: boulag@rocketmail.com, medeni.doc@gmail.com).

This technique is a method of decoding by syndrome, using the theory of error correcting codes, especially linear codes (see [2, 3]). Steganography has taken the concepts associated to error correcting codes and to decoding by syndrome but the use has been reversed.

This work is organized as follows. Sections 2 and 3 present the correspondence between the error-correcting codes and steganographic protocols. In section 4, we recall some properties of linear steganographic protocols. We build our approach in section 5.

2. Steganographic protocol

Definition 2.1. *Let n, k and ρ are three positive integers such that $k \leq n$. A steganographic protocol $\mathfrak{S}$ over an alphabet A to hide messages of length k (secret words) in words of length n (cover words) by modifying at most ρ coordinates(covering radius) is a pair of maps $\mathfrak{S} = (e, r)$ satisfying:*

- $e : A^n \times A^k \to A^n$,
- $r : A^n \to A^k$,
- $\forall (x, s) \in A^n \times A^k : r(e(x, s)) = s$,
- $\forall (x, s) \in A^n \times A^k : d_H(x, e(x, s)) \leq \rho$,

n, k and ρ are the parameters of the steganographic protocol $\mathfrak{S}$.

Maps e and r are respectively called embedding and extraction maps of the steganographic protocol $\mathfrak{S}$. Such a protocol is called a (n, k, ρ)-steganographic protocol $\mathfrak{S}$.

Example 2.2. *Let s and x be the secret word to hide and the cover word respectively. We may suppose that those two words are a sequences of symbols of a finite alphabet A. Let be $s = (s_1, s_2, \cdots, s_k)$ and $x = (x_1, x_2, \cdots, x_n)$, so $s \in A^k$ and $x \in A^n$.*

Let consider the two following maps :

$$e : A^n \times A^k \to A^n$$

and

$$r : A^n \to A^k$$

defined by

$$e((x_1, x_2, \cdots, x_n), (s_1, s_2, \cdots, s_k)) = (x_1, x_2, x_3, \cdots, x_{n-k}, s_1, s_2, \cdots, s_k)$$

and

$$r(x_1, x_2, x_3, \cdots, x_n) = (x_{n-k}, x_{(n-k)+1}, \cdots, x_n).$$

Then (e, r) is a (n, k, k)-steganographic protocol over A.

Definition 2.3. *We call radius of a protocol (e, r) the number*

$$\rho := max\{d(x, e(x, s)), s \in A^k, x \in A^n\}.$$

Remark 2.4. *A good protocol (n, k, ρ)-steganographic (e, r) must satisfies two main requirements:*

1. *The two maps e and r are effective,*
2. *(n, k, ρ) are good parameters such that:*

- $\frac{k}{n}$ *is the greatest possible,*
- $\frac{\rho}{n}$ *is the smallest possible.*

Definition 2.5. *A good protocol steganographic (e, r) of length n is said to be proper if : the embedding map e is such that:*

$e(x, s)$ *is the nearest element to x belonging to $r^{-1}(s) = \{y \in A^n / r(y) = s\}$ (with respect to the hamming distance over A^n, where A denote the alphabet of the protocol).*

Proposition 2.6. *If a steganographic protocol (e, r) is proper then the covering radius ρ is given by:*

$$\rho = max\{d(x, r^{-1}(s))/s \in A^k \text{ and } x \in A^n\}.$$

Proof. Since the protocol is proper then :
$\forall x \in A^n$ and $\forall s \in A^k$ if $e(x, s) = v$ then $d_H(x, v) = min\{d(x, y)/y \in r^{-1}(s)\} = d(x, r^{-1}(s))$.
Since that $\rho := max\{d(x, e(x, s))/s \in A^k, x \in A^n\}$ we have $\rho = max\{d(x, r^{-1}(s)), s \in A^k \text{ and } x \in A^n\}$. □

2.1. The steganographic protocol F_5

The protocol F_5 over the Galois field $\mathbb{F}_2$ permits to hide messages of length k (secret words) in words (cover words) of length $n = 2^k - 1$ by changing more than one of them (i.e. protocol of type $(2^k - 1, k, 1)$). Let $< m >_2$ be the binary expression of m with k bits (so we can consider that $< m >_2$ is in $\mathbb{F}_2^k$). Conversely, for $z \in \mathbb{F}_2^k$ let $< z >_{10}$ be the integer which has z as binary expression, then $1 \leq < z >_{10} \leq 2^k - 1$. Finally, let $\mathbf{e}_i$ be the i^{th} vector of the canonical basis of $\mathbb{F}_2^{2^k-1}$; $\mathbf{e}_0 = 0$. Let consider

i) The map $\gamma : \mathbb{F}_2^{2^k-1} \times \mathbb{F}_2^k \to \mathbb{N}$

$$(x, s) \to \gamma(x, s) =< s + \sum_{i=1}^{2^k-1} x_i < i >_2 >_{10}.$$

ii) Maps e and r defined by :

$$e : \mathbb{F}_2^{2^k-1} \times \mathbb{F}_2^k \to \mathbb{F}_2^{2^k-1},$$
$$(x, s) \to e(x, s) = x + \mathbf{e}_{\gamma(x,s)}.$$
$$r : \mathbb{F}_2^{2^k-1} \to \mathbb{F}_2^k,$$
$$x \to r(x) = \sum_{i=1}^{2^k-1} x_i < i >_2.$$

Let show that (e, r) is a steganographic protocol, or let show that $r(e(x, s)) = s$, for any $s \in \mathbb{F}_2^k$ and for any $x \in \mathbb{F}_2^{2^k-1}$.

Indeed,

1. $r(e(x, s)) = r(x + \mathbf{e}_{\gamma(x,s)})$, we put $j = \gamma(x, s) =< s + \sum_{i=1}^{2^k-1} x_i < i >_2 >_{10}$ then
$$< j >_2 = s + \sum_{i=1}^{2^k-1} x_i < i >_2 : \quad (*)$$
2. $r(x+\mathbf{e}_j) = r(x_1, x_2, \cdots, x_{j+1}, \cdots, x_n) = \sum_{i=1, i\neq j}^{2^k-1} x_i < i >_2 + x_{j+1} < j >_2$, changing $< j >_2$ by its expression given in $(*)$ we obtain : $r(x+\mathbf{e}_j) = s$ so $r(e(x, s)) = s$. Therefore $F5$ is a steganographic protocol.

Remark 2.7.

- *Insert a message s by F_5 in a covering x consists to change the coordinate number $\gamma(x, s)$.*
- *Extraction consists to add all products of each component to the value of the binary expression of the index. i.e : $r(x) = \sum_{i=1}^{2^k-1} x_i < i >_2$*

2.2. Example of application for F_5

For $n = 7$, $k = 3$, how to insert $s = 011$ in $x = 1100101$. i.e. How to calculate $e(011, 1100101)$.
$\gamma(1100101, 011) =< 011 + \sum_{i=1}^{7} x_i < i >_2 >_{10}$
$=< 011 + (1.(001) + 1.(010) + 1.(101) + 1.(111)) >_{10} =< 010 >_{10} = 2$.

Since $s = 011$ and $x = 1100101$ then to insert s in x consists in changing the position number 2 of x from 1 to 0, i.e. $e(x, s) = e(1100101, 011) = 1000101 = v$.

How to extract the message hidden s in the message $v = 1000101$?

I.e. How to calculate $r(1000101)$. By applying the second point of the previous remark we get that $r(v) = r(1000101) = (1.(001) + 1.(101) + 111) = 011 = s$.

3. Codes defined by a steganographic protocol

Recall that a correcting code of length n on alphabet A is a subset of A^n, and the covering radius ρ of a correcting code satisfies $\forall x = (x_1, ..., x_n) \in A^n$:

$$d_H(x, C) = min_{c \in C} d_H(x, c) = min_{c=(c_1,...,c_n) \in C} |\{i : x_i \neq c_i\}| \leq \rho.$$

We denote $(n, \mid C \mid)_\rho$ the parameters of a such code. When C is linear over $\mathbb{F}_q$ of cardinality $\mid C \mid = q^k$ with k is the dimension of the code, we use the notation $[n, k]_\rho$ to say that the parameters of the linear code C are $(n, q^k)_\rho$.

Let $\Upsilon = (e, r)$ be a steganographic protocol. The protocol Υ define a collection F_Υ of correcting codes defined by:

$$F_\Upsilon = \{C_s := r^{-1}(s), s \in A^k\}$$

To decode a word $x \in A^n$ according to the code $C_s = r^{-1}(s)$ of the collection F_Υ, we proceed in this way: If ρ is the radius of Υ then there exists a word x' satisfying:

$$d(x, x') \leq \rho \text{ and } r(x') = s.$$

Then $r(e(x, s)) = s$ which means that $e(x, s)$ is a word decoding x relative to the code C_s.

3.1. Construction of steganographic protocols

To build a steganographic protocol of parameters (n, k, ρ) on an alphabet A, one way is to start by building a surjective map $r : A^n \to A^k$, which map r define a family $F_r := \{C_s = r^{-1}(s) \mid s \in A^k\}$ of codes on A of length n. Then the embedding map e such that (e, r) is a steganographic protocol of parameters (n, k, ρ) is defined by:

For $s \in A^k$ denote $e(s, -)$ the decoding map, defined by the nearest word, associated to the code $C_s = r^{-1}(s)$. Then $e(x, s) = x' \in C_s$, with $d_H(x, x') = d_H(x, C_s) := min\{d_H(x, y), y \in C_s\}$.

Example 3.1. *To build a steganographic protocol of parameters* $(3, 2, 2)$ *on* $\mathbb{F}_2$*, start with given a surjective function* $r : \mathbb{F}_2^3 \to \mathbb{F}_2^2$.
If $r : \mathbb{F}_2^3 \to \mathbb{F}_2^2$ *is such that:*

$$r^{-1}(00) = \{000, 100\}$$
$$r^{-1}(01) = \{010, 001\}$$
$$r^{-1}(10) = \{110, 100\}$$
$$r^{-1}(11) = \{101, 111\},$$

then $C_{00} = \{000, 100\}$*;* $C_{01} = \{010, 001\}$ *;* $C_{10} = \{110, 100\}$ *;* $C_{11} = \{101, 111\}$.

So, $C_{00} = r^{-1}(00)$ *;* $C_{01} = r^{-1}(01)$ *;* $C_{10} = r^{-1}(10)$ *;* $C_{11} = r^{-1}(11)$.
Therefore $e(000, -) : \mathbb{F}_2^3 \to \mathbb{F}_2^3$ *satisfies* $e(000, 00) = 000$*, since* $d(000, x') = d(000, C_{00}) = 0$*. More generally:*

$$e : \mathbb{F}_2^3 \times \mathbb{F}_2^2 \to \mathbb{F}_2^3$$
$$(x, s) \to e(x, s) = d(x, C_s),$$

if $s = 10$ *and* $x = 101$ *then we have* $d(101, C_{10}) = d(101, \{110, 100\}) = 2$ *and* x' *can be* 110 *or* 011*, since* $d(110, 101) = 2$ *and* $(011, 101) = 2$.

Proposition 3.2. *The best steganographic protocol of parameters* (n, k, ρ) *and of extraction map* r *on an alphabet* A*, is one that has as embedding map the map* e *defined by:*

$$(\forall x \in A^n)(\forall s \in A^k)[e(x, s) = x'$$

with $d_H(x, x') = d_H(x, r^{-1}(s))]$.

Lemma 3.3. *A map* $r : A^n \to A^k$ *is an extraction map of a* $[n, k]$*-steganographic protocol if and only if* r *is surjective.*

Proof. Indeed if $r : A^n \to A^k$ is an extraction function of a $[n, k]$-steganographic protocol then for all $x \in A^n$ we have $r \circ e(x, .) = I_{A^k}$ so r is surjective. If $r : A^n \to A^k$ is surjective then from the subsection, Construction of steganographic protocols, there exists an embedding map e such that (e, r) is a steganographic protocol of parameters (n, k, ρ). □

For all $t \in I\!R$ and for all $x_0 \in A^n$ put $B(x_0, t) = \{y \in /d_H(x_0, y) \leq t\}$.

Lemma 3.4. *For all* (n, k, ρ)*-steganographic protocol* (e, r) *over an alphabet* A *and for all* $x_0 \in A^n$ *the map* $r_{/B(x_0,\rho)}$*, the restriction of* r *to the ball* $B(x_0, \rho)$*, is surjective. or,*

$$r_{/B(x_0,\rho)} : B(x_0, \rho) \to A^k$$

$$y \to r(y),$$

is a surjective map.

Proof. The map $r_{/B(x_0,\rho)}$ is well defined.

Let consider $s \in A^k$, since e is the embedding map of the (n, k, ρ)-steganographic protocol (e, r), then $d(x_0, e(s, x_0)) \leq \rho$. Let $y = e(x_0, s)$ then $d(x_0, y) \leq \rho$ and $r(y) = r(e(x_0, s)) = s$. That proves the existence of $y \in B(x_0, \rho)$ such that $r_{/B(x_0,\rho)}(y) = s$. □

It is know that the cardinal of a ball $B(x_0, \rho)$ of A^n is independent from it's center x_0 and it is often denoted by $V_q(n, \rho)$ if q is the cardinal of the alphabet A.

Corollary 3.5. *For all* (n, k, ρ)*-steganographic protocol over an alphabet* A *with* q *elements we have :* $q^k \leq V_q(n, \rho)$

Proof. The map $r_{/B(x_0,\rho)}$ is surjective and then we have

$$Card(\mathbb{F}_q^k) \leq B_n(n, \rho) = V_q(n, \rho).$$

Therefore

$$q^k \leq V_q(n, \rho).$$

□

4. Linear steganographic protocol

Definition 4.1. *A steganographic protocol $\Upsilon = (e, r)$ is called linear if the extraction map r is linear.*

Consequence:
$C_0 := ker(r) = r^{-1}(0_{\mathbb{F}_q^k})$ is a subspace vector of the $\mathbb{F}_q$-space vector $\mathbb{F}_q^n$. So it is a linear code of length n and its dimension is $n-k$. C_0 is called the principal code associated to the steganographic protocol Υ. So

$$F_\Upsilon = \{C_s \mid s \in \mathbb{F}_q^k\} = \mathbb{F}_q^n/C_0 := \{x + C_0 \mid x \in \mathbb{F}_q^n\}.$$

Definition 4.2. *We call an extraction matrix of a steganographic protocol a control matrix of its principal code. Or, an extraction matrix of a steganographic protocol is a matrix associated to the extraction linear map e of this protocol.*

Proposition 4.3. *For each linear steganographic protocol Υ of parameters (n, k, ρ) correspond a linear $[n, n-k]$-code $C(= C_0)$ which has as a control matrix the control matrix of the extraction map of Υ.*

Proposition 4.4. *For each linear code C of, length n, dimension $n-k$ and a control matrix H, correspond an appropriate linear steganographic protocol which has, the mapping r associated to H as an extraction map and (n, k, ρ) as parameters, where ρ denote the covering radius of this code C.*

Proof. For each $a \in \mathbb{F}_q^n$ the map (translation):

$$\begin{aligned} \tau_a : \mathbb{F}_q^n &\to \mathbb{F}_q^n \\ x &\to \tau_a(x) = x + a \end{aligned}$$

is a bijection which conserve the Hamming distance (isometry). Indeed it is clear that τ_a is bijective and that $d(x, y) = d(\tau_a(x), \tau_a(y)) = d(x + a, y + a)$ since the code is linear $d(x, y) = wt(x - y)$. From where $d(\tau_a(x), \tau_a(y)) = wt(\tau_a(x) - \tau_a(y)) = wt(x - y) = d(x, y)$. More r is onto (because its associated matrix is a control matrix of a linear code) therefore Lemma 3.3 implies that there is a $[n, k]$-linear steganographic protocol Υ which has an extraction map r such that $C_\Upsilon : C_0 = C$. It is also true that for all $s \in \mathbb{F}_q^k$ there is $y_s \in \mathbb{F}_q^n$ such that $C_s = y_s + C$ therefore $r(y_s) = s$.

$\rho := max\{d(x, C) \mid x \in \mathbb{F}_q^n\} = max\{d(x, C_0) \mid x \in \mathbb{F}_q^n\}$
$= max\{d(x + y_s, C_0 + y_s) \mid x \in \mathbb{F}_q^n\}$
$= max\{d(\tau_{y_s}(x), C_s) \mid x \in \mathbb{F}_q^n\} = max\{d(x', C_s) \mid x' \in \mathbb{F}_q^n\} = \rho_s$.

So $\rho(\Upsilon) = max_{s \in \mathbb{F}_q^k} \rho_s = max\rho = \rho$. □

5. Construction of linear protocols

To construct a (n, k) - linear steganographic protocol Υ, just consider a matrix H of type $(k \times n)$ and rank k. This matrix H is the extraction matrix of a protocol Υ and at the same time the extraction matrix of the map of this protocol Υ. It is also true that H is the control matrix of the code C_Υ associated to the protocol Υ.

5.1. Decoding a linear code by syndrome

Let C be a $[n, n-k]$- linear code of control matrix $H \in M_{k \times n}(\mathbb{F}_q)$ for each $x \in \mathbb{F}_q^n$, we define the syndrome of x by the quantity $S(x) = x \times H^t$. The decoding method by syndrome associated to the code C consists to : if y is a received word and if I_y is the word of smallest weight in $y + C$, then y is decoded by $x = y - I_y$.

5.2. Embedding algorithm associated to a linear steganographic protocol

Let r be the extraction map of a linear steganographic protocol Υ and let $C_\Upsilon = r^{-1}(0)$, be "the principal linear code associated to Υ". To calculate $e(x,s)$,(if x is a covering word and s is a message to hide in x) if e denote the embedding map associated to the protocol Υ, one way is :

Needed : a coset decoding algorithm: input a syndrome u, output: a coset leader l_u.
Input : a cover x of size n and a message s of size k.
Output : $x' = e(x,s)$, a steganographic cover of s with distortion $d(x,x')$ as small as possible.

- Compute $u := r(x) - s$,
- set $c := x - l_u$,
- $e(x,s) := c$.

Then e is the embedding map of the system Υ. Indeed :

$$r(e(x,s)) = r(c) = r(x - l_u) = r(x) - r(l_u) = u + s - u = s$$

Remark 5.1. *The linear codes which has a fast and effective decoding algorithm, can be used to construct perform embedding algorithm. So these correcting codes are good tools to construct steganographic protocol. The terminals of the parameters of these codes can be translated into terminal parameters of their protocols steganographic associates. All control matrices associated with a linear code give steganographic protocols of same parameters* (n,k,ρ).

5.3. The average symbols modified by a protocol

Upon embedding a message by steganographic protocol Υ, the number of bits modified in a cover word is bounded but not determined, by the covering radius ρ.

Definition 5.2. *Let* $[\Upsilon = (e,r)]$ *be a* (n,k)*-protocol on an alphabet* A *of cardinal* q *with all secret words* s *and cover words* x *have the same probability. We call average symbols modified by* Υ *the umber* $\alpha(\Upsilon)$ *given by the formula :*

$$\alpha(\Upsilon) = \frac{1}{q^{k+n}} \sum_{s\in A^k} \sum_{x\in A^n} d(x, e(x,s))$$

Lemma 5.3. *Let* $\Upsilon = (e,r)$ *be an appropriate* (n,k)*-steganographic protocol on* $\mathbb{F}_q$ *associate to the linear code* C *then :*

$$\alpha(\Upsilon) = \frac{1}{q^n} \sum_{x\in\mathbb{F}_q^n} d(x,C)$$

Proof. Since $e(x,s) = y$ then $d(x,y) = inf\{d(x,c) \mid c \in C_s\}$. Let l_s be a word of smallest weight in C_s then $y = x + l_s$ et $e(x,s) = x + l_s$, so $d(x,e(x,s)) = d(x,x+l_s)$, and since $d(x,x+l_s) = d(x,l_s+C)$ then $d(x,e(x,s)) = d(x-l_s,C)$, from where $\sum_{x\in\mathbb{F}_q^n} d(x,l_s+C) = \sum_{x\in\mathbb{F}_q^n} d(x-l_s,C) = \sum_{z\in\mathbb{F}_q^n} d(z,C)$. Therefore

$$\alpha(\Upsilon) = \frac{1}{q^{n+k}} \sum_{s\in\mathbb{F}_q^k} \sum_{z\in\mathbb{F}_q^n} d(z,C) = \frac{q^k}{q^{n+k}} \sum_{z\in\mathbb{F}_q^n} d(z,C) = \frac{1}{q^n} \sum_{z\in\mathbb{F}_q^n} d(z,C)$$

□

Lemma 5.4. *Let $\Upsilon = (e, r)$ be a (n, k)-steganographic protocol on $\mathbb{F}_q$ associated to a Linear code C. For $i = 0, 1, \cdots, n$ denote α_i the number of representatives of the i weight classes compared to the code C then $\alpha(\Upsilon) = \frac{1}{q^k} \sum_{i=1}^{n} i.\alpha_i$*

Proof. We have $d(x, e(x, s)) = d(x, x + l_s) = w(l_s)$ so,
$\sum_{s\in\mathbb{F}_q^k} \sum_{x\in\mathbb{F}_q^n} d(x, e(x, s)) = \sum_{s\in\mathbb{F}_q^k} \sum_{x\in\mathbb{F}_q^n} w(l_s) = q^n \sum_{s\in\mathbb{F}_q^k} w(l_s)$, or,
$\frac{1}{q^{n+k}} \sum_{s\in\mathbb{F}_q^k} \sum_{z\in\mathbb{F}_q^n} d(x, e(x, s)) = \frac{1}{q^k} \sum_{s\in\mathbb{F}_q^k} w(l_s) = \frac{1}{q^k}(w(l_{s_1}), w(l_{s_2}), \cdots, w(l_{s_{q^k}}))$ □

6. Comparative tables

In this section we present a new family of linear steganographic systems from the family of binary codes, 3-error-correcting primitive BCH codes and we give a comparative study in tables, between the new family, the family of systems presented by C. Manuera in [7] and one studied by A. Westfeld in [8].

A. Westfeldt in [8], studied the family of linear steganographic systems F_5, associated to the family of Hamming binary linear error correcting codes. To a code C of this family of codes, the dimension is $2^m - m - 1$ and a such code is of parameters $[2^m - 1, 2^m - m - 1, 1]$. The parameters of a linear steganographic system of this family are of the form $(2^m - 1, 2m, 3)$. From where the following table:

Table 1. The parameters of F5 [8], $\rho = 1$, $t = 1$.

code	m	n	$k^{'} = n - k$	ρ	$\frac{k'}{n}$	$\frac{\rho}{n}$	$(n, k^{'}, \rho)$
Hamming	4	15	4	1	0.266	0.066	(15,4,1)
Hamming	5	31	5	1	0.161	0.032	(31,5,1)
Hamming	6	63	6	1	0.095	0.015	(63,6,1)
Hamming	7	127	7	1	0.055	0.007	(127,7,1)
Hamming	8	255	8	1	0.031	0.003	(255,8,1)

C. Munuera in [7], presents the family of binary linear error correcting primitive BCH codes, consisting of the quasi perfect codes which are 2-correcting and of length $n = 2^m - 1$. Because these codes are quasi-perfect then their radius of coverage is 3. For a code C of this family of codes, its dimension is $2^m - 2m - 1$ and a such code is of parameters $[2^m - 1, 2^m - 2m - 1, 5]$. Thus each code C of this family of codes, is associated with a linear steganographic protocol of parameters $(2^m - 1, 2m, 3)$. From where the following table:

Table 2. BCH codes [7], $\rho = 3$, $t = 2$.

code	m	n	$k^{'} = n - k$	ρ	$\frac{k'}{n}$	$\frac{\rho}{n}$	$(n, kk^{'}, \rho)$
BCH	4	15	8	3	0.533	0.2	(15,8,3)
BCH	5	31	10	3	0.322	0.096	(31,10,3)
BCH	6	63	12	3	0.190	0.047	(63,12,3)
BCH	7	127	14	3	0.11	0.023	(127,14,3)
BCH	8	255	16	3	0.062	0.011	(255,16,3)

The family of binary linear error correcting codes we offer to study is that of the 3- error-correcting primitive BCH codes. Each code of this family is of length $n = 2^m - 1$ for a non-zero integer m, the covering radius of a such code is 5 ([1], [4] and [5]). Also for a such code C the number of the elements of $\mathbb{F}_2^n/C$ is equal to:

- 2^{3m}, if $m \geq 5$ and then C has $[2^m - 1, 2^m - 1 - 3m, 3]$ as parameters.
- $2^{\frac{5m}{2}}$ if $m = 4$ and then has $[15, 5, 3]$ as parameters,
(Mac Williams and Sloane [[6], p.262].

Thus for each code C of this family is associated to a linear steganographic protocol of parameters:
- $(2^m - 1, 3m, 5)$, if $m \geq 5$.
- $(15, 10, 3)$, if $m = 4$.

From where the following table:

Table 3. BCH primitive codes, $\rho = 5$, $t = 3$.

code	m	n	$k^{'} = n - k$	ρ	$\frac{k'}{n}$	$\frac{\rho}{n}$	$(n, k^{'}, \rho)$
BCH	4	15	10	5	0.6666	0.333	(15,10,5)
BCH	5	31	16	5	0.516	0.161	(31,16,5)
BCH	6	63	45	5	0.714	0.079	(63,45,5)
BCH	7	127	106	5	0.834	0.039	(127,106,5)
BCH	8	255	231	5	0.905	0.119	(255,231,5)

7. Conclusion

In this work, we presented a correspondence between the steganographic systems and error-correcting codes, and we have explained that this correspondence is one to one between linear steganographic systems and linear error correcting codes. We gave some relationships between the parameters and concepts associated to linear steganographic systems, and those of the linear error correcting codes to which they correspond (control matrix covering radius, ...). As the error correcting codes are quite well known, we showed that this correspondence can be used to build good steganographic protocols and to study their properties. We also presented a new steganography based on primitive 3-error correcting BCH codes. Our new protocol, shows that we are able to improve some previous results and suggest new sets of parameters for binary linear steganographic systems. In particulary for steganographic systems of high incorporation rate.

References

[1] E. Assmus, H. Mattson, Some 3–error–correcting BCH codes have covering radius 5, IEEE Trans. Inform. Theory 22(3) (1976) 348–349.
[2] R. Crandall, Some notes on steganography, available at http://dde.binghamton.edu/download/ Crandall_matrix.pdf, 1998.
[3] J. Fridrich, D. Soukal, Matrix embedding for large payloads, IEEE Trans. Inf. Forensics Security 1(3) (2006) 390–395.
[4] T. Helleseth, All binary 3–error–correcting BCH codes of length $2^m - 1$ have covering radius 5, IEEE Trans. Inform. Theory 24(2) (1978) 257–258.
[5] J. van der Horst, T. Berger, Complete decoding of triple–error–correcting binary BCH Codes, IEEE Trans. Inform. Theory 22(2) (1976) 138–147.
[6] F. J. Mac Williams, N. Sloane, The Theory of Error Correcting Codes, Amsterdam, Netherlands, North–Holland, 1966.

[7] C. Munuera, Steganography and error–correcting codes, Signal Process. 87(6) (2007) 1528–1533.
[8] A. Westfeld, F5—A Steganographic Algorithm, Lecture Notes in Comput. Sci. 2137 (2001) 289–302.